

Buenas prácticas en el trabajo colaborativo

Información proporcionada por el Servicio de Seguridad de la Información, D. G. de Telecomunicaciones y Transformación Digital (C. Fomento y Medio Ambiente)



Tanto en las instalaciones habituales de tu centro directivo como fuera de las mismas, se deberán tener previstos procedimientos organizativos que impidan que el trabajo deje de realizarse con regularidad –sobre todo en ausencias programadas-, sin contravenir las políticas de seguridad y las políticas y normas de uso existentes.

Cuentas: En cualquier situación tanto habitual como excepcional, para colaborar no necesitas la identificación de acceso de otras personas, ni compartir tus cuentas con terceros. Se sigue siendo responsable de la custodia y uso de las credenciales asignadas.

Unidades compartidas: Con carácter general dispones de una serie de unidades de red para trabajar en equipo dentro de tu Servicio o tu edificio:

- La unidad del departamento en la que puedes compartir información con los compañeros de Servicio (generalmente unidad G). Existe la posibilidad de crear espacios específicos para las secciones.

- La unidad corporativa de toda la Consejería o edificio al que perteneces (unidad J). Toda la Consejería tiene acceso a la información depositada en esta unidad. Periódicamente se borra su contenido para renovar el espacio disponible.

Unidad individual: Tu Unidad N está ubicada en la infraestructura de la ACCYL, y de ella se realizará copia de seguridad. No introduces información para fines personales en este espacio.



MAYO 2020



Ubica el trabajo colaborativo en los recursos compartidos, y no en esta unidad individualizada a la que sólo tú tienes acceso.

Correo: Puedes organizar el trabajo durante tus ausencias programadas mediante el correo, indicando un mensaje de respuesta automática con información útil para no paralizar los procedimientos. También existe la posibilidad de redirigir los correos recibidos, a otra dirección -siempre corporativa- de un compañero.

Como habitual buena práctica, pon en copia a compañeros que intervengan en trámites compartidos.

Listas de distribución: Tienes a tu disposición las listas o grupos de distribución, para la gestión y comunicación de correos con información que deba ser rápidamente gestionada; se tiene que solicitar y el departamento correspondiente evaluará la necesidad de la petición. Llimita, eso sí, su utilización y sus participantes.

Dispositivos: Utiliza las impresoras, escáneres, etc... de red informática, evitando aquellos conectados directamente a un equipo concreto. De este modo, se podrá acceder a estos dispositivos desde cualquier puesto.

Recuerda que con tu cuenta ACCyL puedes iniciar sesión en cualquier equipo para utilizarlo sin solicitar otras credenciales.

Herramientas externas: Utiliza exclusivamente las herramientas colaborativas que la ACCyL ha puesto a disposición de sus empleados, como puede ser la nube propia **JCyLTransfer**, o el sistema de mensajería corporativo, etc.

Cualquier herramienta externa no autorizada, no tiene soporte por tu CAU y puede provocar una brecha de seguridad conllevando exfiltración de datos, en especial subiendo información no cifrada y sin requerir permisos de acceso.

MAYO 2020

Videoconferencias: No generes y compartas públicamente enlaces o convocatorias de reuniones virtuales, limitando su acceso con contraseña al número de convocados necesarios. Toda reunión tendrá un moderador para gestionar las características como cámaras y micrófonos abiertos o cerrados, grabación de la sesión, posibilidad de compartir contenidos, etc. Cuida tu fondo de imagen.

Soportes: Evita guardar información laboral en soportes extraíbles, son poco útiles para el trabajo a distancia de larga duración, y pueden perderse con datos confidenciales o de carácter personal. No conectes dispositivos USB sospechosos, sobre todo no proporcionados por la ACCyL, y únicamente con autorización previa cuando sea imprescindible para la realización de tus funciones.

Aplicaciones: La mayoría de las aplicaciones o servicios, también de terceros, contienen datos personales y mantienen ficheros de acciones realizadas y de

históricos. Solicita cuentas de aplicación para cada una de las personas que necesiten acceder a las mismas, mediante los procedimientos aprobados y de forma habitual a través de solicitud a tu CAU.

Si eres empleado público de la Junta de Castilla y León el uso de medios digitales deberá realizarse conforme a la [política de seguridad](#) de la ACCyL, así como la política de uso de los [servicios de comunicaciones e informática](#) para todo usuario de los mismos.



Descubre más conceptos sobre buenas prácticas en el trabajo colaborativo.

